

Exhibit 36

**Excerpts of Eric Quitugua
Investigative Testimony Transcripts**

C-08755

***Quitugua, Eric - Vol.
I.20210831.344327-C***

8/31/2021 9:58 AM

Condensed Transcript

Prepared by:

Lory Stone
C-08755

Sunday, October 10, 2021

Page 1	Page 3																																														
<p>1 THE UNITED STATES SECURITIES AND EXCHANGE COMMISSION</p> <p>2</p> <p>3 In the Matter of:)</p> <p>4) File No. C-08755-A</p> <p>5 SOLARWINDS CORPORATION)</p> <p>6)</p> <p>7 WITNESS: Eric Quitugua</p> <p>8 PAGES: 1 through 225</p> <p>9 PLACE: Securities and Exchange Commission</p> <p>10 175 West Jackson Blvd</p> <p>11 Chicago, Illinois</p> <p>12 DATE: Tuesday, August 31, 2021</p> <p>13</p> <p>14 The above-entitled matter came on for hearing, via</p> <p>15 WebEx, pursuant to notice, at 9:58 a.m.</p> <p>16</p> <p>17</p> <p>18</p> <p>19</p> <p>20</p> <p>21</p> <p>22</p> <p>23</p> <p>24 Diversified Reporting Services, Inc.</p> <p>25 (202) 467-9200</p>	<p>1 APPEARANCES(CONT.):</p> <p>2</p> <p>3 Also Present:</p> <p>4</p> <p>5 Jason Winds, SolarWinds EVP and Chief</p> <p>6 Administrative Officer</p> <p>7 Becky Melton, SolarWinds, VP of Legal</p> <p>8 Era Calhoun, SEC Paralegal</p> <p>9</p> <p>10</p> <p>11</p> <p>12</p> <p>13</p> <p>14</p> <p>15</p> <p>16</p> <p>17</p> <p>18</p> <p>19</p> <p>20</p> <p>21</p> <p>22</p> <p>23</p> <p>24</p> <p>25</p>																																														
Page 2	Page 4																																														
<p>1 APPEARANCES:</p> <p>2</p> <p>3 On behalf of the Securities and Exchange Commission:</p> <p>4 WILLIAM NEY, ESQ., Senior Counsel</p> <p>5 LORY STONE, ESQ., Senior Counsel</p> <p>6 BENJAMIN BRUTLAG, ESQ., Senior Counsel</p> <p>7 MICHAEL BAKER, ESQ., Senior Counsel</p> <p>8 KENNETH ZAVOS, IT Forensics Specialist</p> <p>9</p> <p>10 Securities and Exchange Commission</p> <p>11 Division of Enforcement</p> <p>12 175 West Jackson Blvd</p> <p>13 Chicago, Illinois</p> <p>14 (202) 551-7612</p> <p>15</p> <p>16 On behalf of the Witness:</p> <p>17 JULIE RIEWE, ESQ.</p> <p>18 ANNA MOODY, ESQ.</p> <p>19 JONATHAN DEMARS, ESQ.</p> <p>20 Debevoise & Plimpton</p> <p>21 801 Pennsylvania Avenue N.W.</p> <p>22 Washington, D.C. 20004</p> <p>23 (202) 383-8070</p> <p>24</p> <p>25</p>	<p>1 C O N T E N T S</p> <p>2</p> <table border="0"> <tr> <td>3 WITNESS</td><td>EXAMINATION</td></tr> <tr> <td>4 Eric Quitugua</td><td>5</td></tr> <tr> <td>5</td><td></td></tr> <tr> <td>6 EXHIBITS:</td><td>DESCRIPTION IDENTIFIED</td></tr> <tr> <td>7 1</td><td>Formal Order 7</td></tr> <tr> <td>8 2</td><td>SEC Form 1662 8</td></tr> <tr> <td>9 3</td><td>Testimony Procedures 12</td></tr> <tr> <td>10 6</td><td>Incident Improvement Plan 6/22/20 23</td></tr> <tr> <td>11 7</td><td>Org Chart 31</td></tr> <tr> <td>12 15</td><td>2H 2019 CTO/DOIT R4R Goals 106</td></tr> <tr> <td>13 17</td><td>Campbell Email to Quitugua 65</td></tr> <tr> <td>14 19</td><td>Quarterly Overview 8/16/19 60</td></tr> <tr> <td>15 31</td><td>8/18/21 Subpoena 13</td></tr> <tr> <td>16 32</td><td>Background Questionnaire 8/18/21 18</td></tr> <tr> <td>17 33</td><td>Q4 2020 QRR 10/27/20 52</td></tr> <tr> <td>18 34</td><td>Quitugua Email to Lyman 9/11/18 121</td></tr> <tr> <td>19 35</td><td>Vulnerability Incident Review 7/20 156</td></tr> <tr> <td>20</td><td></td></tr> <tr> <td>21</td><td></td></tr> <tr> <td>22</td><td></td></tr> <tr> <td>23</td><td></td></tr> <tr> <td>24</td><td></td></tr> <tr> <td>25</td><td></td></tr> </table>	3 WITNESS	EXAMINATION	4 Eric Quitugua	5	5		6 EXHIBITS:	DESCRIPTION IDENTIFIED	7 1	Formal Order 7	8 2	SEC Form 1662 8	9 3	Testimony Procedures 12	10 6	Incident Improvement Plan 6/22/20 23	11 7	Org Chart 31	12 15	2H 2019 CTO/DOIT R4R Goals 106	13 17	Campbell Email to Quitugua 65	14 19	Quarterly Overview 8/16/19 60	15 31	8/18/21 Subpoena 13	16 32	Background Questionnaire 8/18/21 18	17 33	Q4 2020 QRR 10/27/20 52	18 34	Quitugua Email to Lyman 9/11/18 121	19 35	Vulnerability Incident Review 7/20 156	20		21		22		23		24		25	
3 WITNESS	EXAMINATION																																														
4 Eric Quitugua	5																																														
5																																															
6 EXHIBITS:	DESCRIPTION IDENTIFIED																																														
7 1	Formal Order 7																																														
8 2	SEC Form 1662 8																																														
9 3	Testimony Procedures 12																																														
10 6	Incident Improvement Plan 6/22/20 23																																														
11 7	Org Chart 31																																														
12 15	2H 2019 CTO/DOIT R4R Goals 106																																														
13 17	Campbell Email to Quitugua 65																																														
14 19	Quarterly Overview 8/16/19 60																																														
15 31	8/18/21 Subpoena 13																																														
16 32	Background Questionnaire 8/18/21 18																																														
17 33	Q4 2020 QRR 10/27/20 52																																														
18 34	Quitugua Email to Lyman 9/11/18 121																																														
19 35	Vulnerability Incident Review 7/20 156																																														
20																																															
21																																															
22																																															
23																																															
24																																															
25																																															

<p style="text-align: right;">Page 133</p> <p>1 would triage that, create tickets, do the follow-up. So 2 depending on which part of the team those assignments 3 went to. 4 Q You referred to SEM. Is that S-I-E-M, just 5 for the court reporter? 6 A Yeah, apologize. It's LEM, Log & Event 7 Manager, was renamed to Security Events Manager so I'll 8 use them interchangeably, LEM, SEM. 9 Q So it's just S-E-M? 10 A Yeah, just S-E-M, yeah. There's also a SIM, 11 sorry. I don't want to confuse, so. 12 Q Got it. So beyond having the change 13 management policies in place, did Solar -- did 14 SolarWinds actually follow or apply those change 15 management guidelines on a daily basis? 16 A Yes. 17 Q Are you aware of any deficiencies in the 18 change management process before -- in the 2018 to 2020 19 time period? 20 A Not that I'm aware of, no. 21 Q Did anyone ever tell you that there were 22 deficiencies in the change management process during 23 that time period? 24 A Not that I can recall, no. 25 Q If you go to the next page, which is -- if you</p>	<p style="text-align: right;">Page 135</p> <p>1 right. These are production systems that are operating 2 and providing the actual services to the end user. In 3 this case, could be the employees. It could be our 4 customers, which if there are application servers that 5 are on the internet, those would be considered 6 production systems. 7 Q Okay. What is the -- what's the development 8 environment? 9 A The development environment is the environment 10 where all the, you know, development and testing of 11 updates and modifications to product code are done. 12 Q So is that separate from the testing 13 environment or not at SolarWinds? 14 A I don't know the answer to that. I know that 15 there is a -- there's two domains at SolarWinds, a DEV 16 Domain and a TUL domain. One is considered production, 17 and one's considered development. 18 Q Okay. And so which one is production? 19 A The TUL domain. 20 Q And when you said "TUL," that's T-U-L? 21 A T-U-L. 22 Q Okay. And the DEV domain, that's the 23 development domain? 24 A Yes. 25 Q And that's D-E-V?</p>
<p style="text-align: right;">Page 134</p> <p>1 go to Page 9, you'll see a section there regarding 2 network security. Do you see that? 3 A Yes, I do. 4 Q All right. In the first -- well, there's 5 several questions. One is environments for development 6 staging, testing, QA, and production supported and 7 maintained. Do you see that? 8 A Yes. 9 Q From a security standpoint, is it important 10 for the development staging, testing, QA, and production 11 environment to be separated? 12 A Yes. 13 Q Why? 14 A So that any changes within the development and 15 staging environments don't affect production systems 16 that could potentially bring down and make them 17 unavailable for -- for the services that they provide. 18 Q And does the production -- the production 19 environment that's described there, is that the 20 environment in which the SolarWinds' products are 21 created or produced or what is -- well, let me just ask 22 this: What is the production environment that's 23 described there? 24 A So production environments are environments 25 where there are strict change management procedures,</p>	<p style="text-align: right;">Page 136</p> <p>1 A Yes. 2 Q Okay. Is that domain sometimes referred to as 3 SWDEV? 4 A Yes. 5 Q Okay. The next question down under this 6 section says, "Are firewalls used to segment network 7 zones and terminate connections to external networks?" 8 Do you see that? 9 A Yes. 10 Q Can you describe that? What is the importance 11 of firewalls segmenting the network zones for 12 cybersecurity purposes? 13 A Sure. So again, firewalls are used to ensure 14 the segmentation so that the appropriate traffic as well 15 as access to resources within that specific zone or 16 network are adequate -- there are adequate security 17 controls that allow access or denial into those specific 18 environments. 19 Q Okay. And so for example, between the DEV and 20 the TUL domains, was there a firewall used to segment 21 those two network zones? 22 A Yes. 23 Q And then it also refers to terminating 24 connections to external networks. Do you see that? 25 A Yes.</p>

<p style="text-align: right;">Page 221</p> <p>1 a pretty -- a pretty large difference between those for 2 a process that was going on. 3 A I think the -- the big thing that we were 4 doing at this time is that we were continuously evolving 5 our processes and continuously improving upon any 6 additional gaps that we were finding, right. So again, 7 I can't speak directly to the timing of whether or not 8 we were already doing the reviews or not during this 9 time. 10 Q Were you finding a lot of gaps? You said that 11 you were going back and you were -- you were identifying 12 gaps to improve on. Did you find a lot of gaps? 13 A Again, from -- as we identified those gaps, we 14 worked with, you know, the VP of security and our CIO, 15 but to put those into some formalized tracking and 16 program. 17 Q Okay. What was the formalized tracking and 18 program? Where is that -- where is that documented -- 19 A So we were -- 20 Q -- reports we've been looking at today? 21 A We reviewed a document called the R4R. Part 22 of those gaps were reflected there as goals and 23 objectives. 24 Q Okay. So things that were goals and 25 objectives there were gaps prior to that time period?</p>	<p style="text-align: right;">Page 223</p> <p>1 you wish to clarify anything or add anything else to the 2 statements you've already made? 3 A No. 4 MR. NEY: Okay. Counsel, do you wish to ask 5 any clarifying questions at this time? 6 MS. RIEWE: I don't think so. Obviously 7 reserve for tomorrow, but we can -- we have the benefit 8 of a second day so we can do it tomorrow. 9 MR. NEY: Yes, any clarifying questions that 10 you want to ask, tomorrow either at the beginning or at 11 the end, let me know. 12 Okay. At this time, we're adjourning the 13 testimony until tomorrow morning. 14 Mr. Quitugua, although your testimony is 15 adjourned, you remain under subpoena, and when we come 16 back tomorrow, I will go ahead and put your under oath 17 again, okay? 18 We are off the record at 4:44 p.m. on August 19 31st, 2021. 20 (Whereupon, at 4:44 p.m., the examination was 21 adjourned.) 22 * * * * * 23 24 25</p>
<p style="text-align: right;">Page 222</p> <p>1 A No, that's not correct. 2 Q Okay. So what were you saying then about the 3 R4Rs? How can that help me identify what the gaps were? 4 A So if we identified a gap, you know, and then 5 we got it through the risk review process, Tim, Rani 6 would say, well, okay, is this a way to improve the 7 overall security posture of the program? And if it was, 8 say okay, well, let's make that as a goal and objective. 9 Part of that was SCIP. Part of that was conducting 10 routine vulnerability assessments, as an example. 11 Q So would the gaps then be identified in the 12 SCIPs and in the QRRs, the quarterly risk reviews? 13 A If you looked at the -- yes, the actions 14 needed in the SCIPs, it was part of that would have 15 resulted from gaps that were identified. 16 Q Okay. 17 So we looked at product management 18 SCIPs before, and there were various actions needed. 19 Those are the things that you would refer -- that you'd 20 be referring to as gaps here? 21 A Yes. 22 Q Okay. Okay. I think that's going to pretty 23 well wrap up what we're going to cover today, Mr. 24 Quitugua. 25 Prior to adjourning your testimony today, do</p>	<p style="text-align: right;">Page 224</p> <p>1 PROOFREADER'S CERTIFICATE 2 3 In the Matter of: SOLARWINDS, INC. 4 Witness: Eric Quitugua 5 File No: C-08755-A 6 Date: Tuesday, August 31, 2021 7 Location: Chicago, Illinois 8 9 This is to certify that I, Christine Boyce, 10 (the undersigned) do hereby certify that the foregoing 11 transcript is a complete, true and accurate 12 transcription of all matters contained on the recorded 13 proceedings of the investigative testimony. 14 15 16 17 18 19 _____ 9-13-2021 20 21 22 23 24 25</p>

REPORTER'S CERTIFICATE

1
2
3 I, Kevin Carr, reporter, hereby certify that the
4 foregoing transcript is a complete, true and accurate
5 transcript of the testimony indicated, held on 8-31-21,
6 at Chicago, IL in the matter of:
7 SOLARWINDS, INC.
8
9 I further certify that this proceeding was recorded by
10 me, and that the foregoing transcript has been prepared
11 under my direction.
12
13
14
15 9-13-2021
16
17
18
19
20
21
22
23
24
25

C-08755

***Quitugua, Eric - Vol.
II.20210901.344328-C***

9/1/2021 9:32 AM

Condensed Transcript

Prepared by:

Lory Stone
C-08755

Sunday, October 10, 2021

<p style="text-align: right;">Page 226</p> <p>1 THE UNITED STATES SECURITIES AND EXCHANGE COMMISSION</p> <p>2</p> <p>3 In the Matter of:)</p> <p>4) File No. C-08755-A</p> <p>5 SOLARWINDS CORPORATION)</p> <p>6)</p> <p>7 WITNESS: Eric Quitugua</p> <p>8 PAGES: 226 through 427</p> <p>9 PLACE: Securities and Exchange Commission</p> <p>10 175 West Jackson Blvd.</p> <p>11 Chicago, Illinois</p> <p>12 DATE: Wednesday, September 1, 2021</p> <p>13</p> <p>14 The above-entitled matter came on for hearing, via</p> <p>15 WebEx, pursuant to notice, at 9:32 a.m.</p> <p>16</p> <p>17</p> <p>18</p> <p>19</p> <p>20</p> <p>21</p> <p>22</p> <p>23</p> <p>24 Diversified Reporting Services, Inc.</p> <p>25 (202) 467-9200</p>	<p style="text-align: right;">Page 228</p> <p>1 APPEARANCES(CONT.):</p> <p>2</p> <p>3 Also Present:</p> <p>4</p> <p>5 Jason Winds, SolarWinds EVP and Chief</p> <p>6 Administrative Officer</p> <p>7 Becky Melton, SolarWinds, VP of Legal</p> <p>8 Era Calhoun, Paralegal</p> <p>9</p> <p>10</p> <p>11</p> <p>12</p> <p>13</p> <p>14</p> <p>15</p> <p>16</p> <p>17</p> <p>18</p> <p>19</p> <p>20</p> <p>21</p> <p>22</p> <p>23</p> <p>24</p> <p>25</p>																																														
<p style="text-align: right;">Page 227</p> <p>1 APPEARANCES:</p> <p>2</p> <p>3 On behalf of the Securities and Exchange Commission:</p> <p>4 WILLIAM NEY, ESQ., Senior Counsel</p> <p>5 LORY STONE, ESQ., Senior Counsel</p> <p>6 BENJAMIN BRUTLAG, ESQ., Senior Counsel</p> <p>7 MICHAEL BAKER, ESQ., Senior Counsel</p> <p>8 KENNETH ZAVOS, IT Forensics Specialist</p> <p>9 Securities and Exchange Commission</p> <p>10 Division of Enforcement</p> <p>11 175 West Jackson Blvd.</p> <p>12 Chicago, Illinois</p> <p>13 (202) 551-7612</p> <p>14</p> <p>15 On behalf of the Witness:</p> <p>16 JULIE RIEWE, ESQ.</p> <p>17 ANNA MOODY, ESQ.</p> <p>18 JONATHAN DEMARS, ESQ.</p> <p>19 Debevoise & Plimpton</p> <p>20 801 Pennsylvania Avenue N.W.</p> <p>21 Washington, D.C. 20004</p> <p>22 (202) 383-8070</p> <p>23</p> <p>24</p> <p>25</p>	<p style="text-align: right;">Page 229</p> <p>1 C O N T E N T S</p> <p>2</p> <table border="0"> <tr> <td>3 WITNESS</td> <td>EXAMINATION</td> </tr> <tr> <td>4 Eric Quitugua</td> <td>230</td> </tr> <tr> <td>5 EXHIBITS: DESCRIPTION IDENTIFIED</td> <td></td> </tr> <tr> <td>6 1 Formal Order</td> <td>231</td> </tr> <tr> <td>7 6 Incident Improvement Plan 6/22/20</td> <td>282</td> </tr> <tr> <td>8 18 Security Compliance 5/17/19</td> <td>310</td> </tr> <tr> <td>9 19 Quarterly Overview 8/16/19</td> <td>326</td> </tr> <tr> <td>10 23 Pierce Email 1/11/18</td> <td>336</td> </tr> <tr> <td>11 25 Q1 2020 QRR 3/3/20</td> <td>319</td> </tr> <tr> <td>12 31 8/18/21 Subpoena</td> <td>231</td> </tr> <tr> <td>13 36 Brown Email 11/19/19</td> <td>264</td> </tr> <tr> <td>14 37 PSIRT Email 11/19/19</td> <td>356</td> </tr> <tr> <td>15 39 Trump Email 4/25/17</td> <td>366</td> </tr> <tr> <td>16 40 Security Team Email 11/6/20</td> <td>370</td> </tr> <tr> <td>17 41 WhiteSource Email 9/8/20</td> <td>386</td> </tr> <tr> <td>18 42 Pierce Email 6/13/18</td> <td>394</td> </tr> <tr> <td>19 43 Esquitin Email 6/5/20</td> <td>398</td> </tr> <tr> <td>20 44 Kanalyanee Email 9/18/20</td> <td>403</td> </tr> <tr> <td>21 46 Confluence RAF 9/3/20</td> <td>409</td> </tr> <tr> <td>22 47 ITOM DOJ Malware Issues</td> <td>414</td> </tr> <tr> <td>23 48 Security Review 6/24/20</td> <td>423</td> </tr> <tr> <td>24 49 Brown-Nels Messaging 12/7/20</td> <td>420</td> </tr> <tr> <td>25</td> <td></td> </tr> </table>	3 WITNESS	EXAMINATION	4 Eric Quitugua	230	5 EXHIBITS: DESCRIPTION IDENTIFIED		6 1 Formal Order	231	7 6 Incident Improvement Plan 6/22/20	282	8 18 Security Compliance 5/17/19	310	9 19 Quarterly Overview 8/16/19	326	10 23 Pierce Email 1/11/18	336	11 25 Q1 2020 QRR 3/3/20	319	12 31 8/18/21 Subpoena	231	13 36 Brown Email 11/19/19	264	14 37 PSIRT Email 11/19/19	356	15 39 Trump Email 4/25/17	366	16 40 Security Team Email 11/6/20	370	17 41 WhiteSource Email 9/8/20	386	18 42 Pierce Email 6/13/18	394	19 43 Esquitin Email 6/5/20	398	20 44 Kanalyanee Email 9/18/20	403	21 46 Confluence RAF 9/3/20	409	22 47 ITOM DOJ Malware Issues	414	23 48 Security Review 6/24/20	423	24 49 Brown-Nels Messaging 12/7/20	420	25	
3 WITNESS	EXAMINATION																																														
4 Eric Quitugua	230																																														
5 EXHIBITS: DESCRIPTION IDENTIFIED																																															
6 1 Formal Order	231																																														
7 6 Incident Improvement Plan 6/22/20	282																																														
8 18 Security Compliance 5/17/19	310																																														
9 19 Quarterly Overview 8/16/19	326																																														
10 23 Pierce Email 1/11/18	336																																														
11 25 Q1 2020 QRR 3/3/20	319																																														
12 31 8/18/21 Subpoena	231																																														
13 36 Brown Email 11/19/19	264																																														
14 37 PSIRT Email 11/19/19	356																																														
15 39 Trump Email 4/25/17	366																																														
16 40 Security Team Email 11/6/20	370																																														
17 41 WhiteSource Email 9/8/20	386																																														
18 42 Pierce Email 6/13/18	394																																														
19 43 Esquitin Email 6/5/20	398																																														
20 44 Kanalyanee Email 9/18/20	403																																														
21 46 Confluence RAF 9/3/20	409																																														
22 47 ITOM DOJ Malware Issues	414																																														
23 48 Security Review 6/24/20	423																																														
24 49 Brown-Nels Messaging 12/7/20	420																																														
25																																															

Page 286

1 TUL or the DEV domain. Do you recall that?
 2 A Yes.
 3 Q And I just wanted to ask so I understand
 4 better. So with -- well, let's focus specifically on
 5 the issue that we were talking about, the concept of
 6 least privileged not being followed on those -- on those
 7 workstations. How can you remediate that if those
 8 workstations are not connected to one of the Active
 9 Directory domains?
 10 A So first thing that we do is identify, and the
 11 way we identify those systems is we run -- you know, we
 12 talked about automated scanning of the corporate
 13 infrastructure. So those are automated scheduled scans.
 14 They'll return whether or not a system that was scanned
 15 is either in a work group or in a domain.
 16 So we'll group those systems in buckets of
 17 work group and which domains they're joined to, and then
 18 that's the list that we go down and work with the
 19 network security or network management teams to
 20 determine first, are they authorized on the network, and
 21 we run through those playbooks. That's -- that's one of
 22 the ways that we find these systems that are not joined
 23 to the domain.
 24 Q Okay. And so that's how you can find the
 25 system that's not joined to the domain. Is there any

Page 287

1 way to -- to remediate the fact that they're not using
 2 the concept of least privileged, though, other than
 3 making them -- putting those systems on the domain?
 4 A Yeah, I mean, we -- we first look at business
 5 justification, right. Our processes say, look, all
 6 systems that are on the network, the managed network,
 7 must be or should be on the domain, right. And so the
 8 first question we ask is, well, what is -- why is it not
 9 joined to any domain? What is the business
 10 justification? And if they -- if one can't be given,
 11 then we work with the system owner to put it on the
 12 domain so it does get the domain policies.
 13 Q Okay. Then so the only way to make sure that
 14 the domain policies are being followed is if you
 15 actually add those workstations to one of the existing
 16 domains?
 17 A It gives the IT groups the ability to control
 18 what policies get enforced, yes.
 19 Q Okay. And if it's not -- if it's not on one
 20 of the domains, you don't have the ability to enforce
 21 that?
 22 A We have the ability to reach out and find who
 23 -- you know, who owns it and then have those subsequent
 24 conversations about, you know, why isn't it on the
 25 domain, those types of things.

Page 288

1 Q Yes. But you can't apply the rules to it if
 2 it's not --
 3 A You can't apply the domain rules, yes.
 4 Q Okay. Looking again at the slide that's in
 5 12273 in Exhibit 36, it's the same slide we had been
 6 looking at before we went to the org chart, there's a
 7 second issue that's identified and says, "The use of
 8 shared accounts throughout internal and external
 9 applications." Can you tell me what that issue refers
 10 to?
 11 A That was specifically addressing service
 12 accounts that were being shared.
 13 Q Is there a security issue relating to the use
 14 of those shared accounts?
 15 A Yes, we talked a little bit about that
 16 yesterday and some of the risks associated with that.
 17 There's no way for -- for teams to identify, you know,
 18 who was the individual using that shared credential.
 19 Q And so that would -- so would that be access
 20 control or an access management issue?
 21 A It would be an item, yes, that needs to be
 22 remediated, yes.
 23 Q Okay. So we had talked -- we had talked about
 24 access -- access control. Let me ask this first. This
 25 slide entitled "Enterprise Access Management," is that

Page 289

1 the same as what you referred to yesterday as access
 2 control?
 3 A I'm not sure I understand the question. Could
 4 you repeat?
 5 Q The top of this slide is entitled "Enterprise
 6 Access Management." Yesterday we looked at a policy or
 7 a guideline that related to access control. Are those
 8 the same thing?
 9 A Yeah, I would say they are, yes.
 10 Q Access management and access control, in your
 11 -- in your mind, those are referring to the same thing?
 12 A In the context of the project, yes. The
 13 access management project dealt with how we improve
 14 access controls as defined in our guidelines.
 15 Q Okay. In the -- so in this early 2018 time
 16 period, why was it that shared accounts were being used
 17 throughout the internal and external applications?
 18 A I'm not sure I understand. Can you repeat one
 19 more time, please?
 20 Q Yeah. So early 2018, and you were saying that
 21 the use of shared accounts was an issue that you
 22 identified in this presentation. I'm just wondering why
 23 was it that shared accounts were being used in time
 24 period?
 25 A So shared accounts, service accounts that were

<p style="text-align: right;">Page 358</p> <p>1 A That means that the credential was not 2 encrypted so any user who was able to access that repo 3 was able to see the credential. 4 Q Okay. And was the repo -- are those repos -- 5 they're part of the public GitHub. So is it your 6 understanding that that repo was publicly available? 7 A Again, based on our investigation of this 8 particular security issue, we did find that the public 9 GitHub repo was owned by the intern. 10 Q Okay. And was it available to members of the 11 public? 12 A It was confirmed that it was available to 13 members of the public. 14 Q Okay. There was no -- no -- no limitations on 15 who had access to it? 16 A I don't recall. No, I don't believe so, not 17 from the investigations we did as part of the security 18 incident. 19 Q And when you refer to credentials, you mean 20 user name and password, correct? 21 A Yes. 22 Q Okay. What is the -- just a moment. There's 23 a reference further down to a FTP URL, and it's 24 SolarWinds.upload.akamai, a-k-a-m-a-i, .com. Do you see 25 that?</p>	<p style="text-align: right;">Page 360</p> <p>1 the password and user name for that Akamai account? 2 A I'm trying to think. I would have to refer to 3 the incident notes. If it was confirmed and validated, 4 it would have been captured in the incident log. 5 Q Okay. Towards the end, the report states that 6 "via this, any hacker could upload malicious exe and 7 update it with released SolarWinds' products." Do you 8 see that? 9 A Yes. 10 Q Is that an accurate statement of the risk 11 presented by this -- by these publicly available 12 credentials? 13 A With -- with those credentials, yes, any -- 14 anybody could upload executables to the repository -- to 15 the Akamai FTP site. 16 Q The password solarwinds123, there's no 17 capitals in that, that is -- that is inconsistent with 18 SolarWinds' password requirements, correct? 19 A Yes, that's correct. 20 Q Is this a system that was outside SolarWinds 21 -- the SolarWinds domain? 22 A This application was not immigrated into 23 Active Directory single sign-on. 24 Q Was that -- that's a better way to state it. 25 And so is that the reason why this password that</p>
<p style="text-align: right;">Page 359</p> <p>1 A Yes. 2 Q What is -- what is Akamai, if you know? 3 A Akamai is our content delivery network 4 provider, a CDN. 5 Q And what does that mean? What is a CDN? 6 A They basically -- we use Akamai as a content 7 distribution point for distributing, you know, our own 8 files and whatnot. They also serve as our DNS, but for 9 this particular purpose, we use them as a CDN. 10 Q When you refer to content distribution point, 11 what -- what kind of content are you referring to being 12 distributed? 13 A In this specific case, access to it was done 14 by FTP. 15 Q Okay. I guess what I don't understand is what 16 content was distributed by SolarWinds through Akamai. 17 Is it -- is it products? Is it product updates? Is it 18 -- what did SolarWinds distribute through Akamai? 19 A Downloads of our -- of our product. 20 Q Okay. The next portion of the -- of the 21 description provided has the user name as SolarWinds, 22 and then it has the password solarwinds123. Do you see 23 that? 24 A Yes. 25 Q Were you able to confirm that that was indeed</p>	<p style="text-align: right;">Page 361</p> <p>1 violated SolarWinds' password policy could be -- could 2 be used for that application? 3 A Yes. 4 Q Okay. If it was part of the Active Directory, 5 then the Active Directory rules would -- would apply to 6 it, correct? 7 A Yes, that is correct. 8 Q Okay. And I think I stated at the -- let me 9 just clarify with you. You would agree, wouldn't you, 10 that solarwinds123 is inconsistent with the -- with 11 SolarWinds' password requirements that we looked at 12 earlier? 13 A Yes. 14 Q Okay. Would you agree that that is a very 15 weak password? 16 A Yes. 17 Q For what reasons? As a cybersecurity 18 professional, what's wrong with solarwinds123 as a 19 password? 20 A You know, numbers in sequence, all lower case, 21 no complexity, uses common names. 22 Q All those things? 23 A Uh-huh. 24 Q Also lack of any special character? 25 A Yes.</p>

<p style="text-align: right;">Page 362</p> <p>1 Q Okay. Was solarwinds123 a password that was 2 used on other systems at SolarWinds? 3 A I want to make sure I understand the question. 4 You're asking if the password used here in the -- as 5 part of this report was used also elsewhere within the 6 organization? 7 Q Yes. Are you aware of solarwinds123 being 8 used as a password in other parts of the organization? 9 A For applications and systems that were drawing 10 to the domain, that would not have been possible because 11 of the group policy enforcements. In our lab 12 environments, there could have -- I'm sorry, no. There 13 may have been the possibility that in the lab 14 environments, passwords such as, you know, weak 15 passwords that were in use. 16 MS. RIEWE: And maybe just to jump in, Eric, I 17 think he's asking you if you know. Anything in the 18 world is possible in theory. So if you know, you know. 19 If you don't, you don't. I think leave it at that so 20 you're not speculating on possibilities. 21 THE WITNESS: Not during this time period, no. 22 BY MR. NEY: 23 Q You're not aware of it being used in others 24 during the time period? 25 A Not during this time, no.</p>	<p style="text-align: right;">Page 364</p> <p>1 previously? 2 A Yes, I have. 3 Q And you don't recall solarwinds123 being the 4 password for that? 5 A I do not recall it being that password, no. 6 Q Do you recall it being used as the password 7 for any servers at SolarWinds? 8 A Not to my knowledge, no. 9 Q As the senior security manager at SolarWinds, 10 do you have access to -- to the passwords that are used 11 for SolarWinds' servers? 12 A I only have access to the credentials that we 13 use to run our vulnerability scanner. 14 Q Okay. The -- does your group provide any sort 15 of auditing or review of the passwords that are used for 16 SolarWinds -- for SolarWinds' servers to make sure 17 they're consistent with the password policy? 18 A I don't recall if we did the checks during 19 this timeframe or not. I don't have any recollection 20 right now if we did or not during this time period. 21 Q Okay. Are there checks that you do now? 22 A Yes. 23 Q During this time period, who would have been 24 responsible for doing those checks, if anyone did? 25 A The IT operations group and the systems</p>
<p style="text-align: right;">Page 363</p> <p>1 Q Okay. Just going back to the possibility that 2 you did address this, what area were you saying that 3 possibility existed in? 4 A Again, we talked about systems that weren't 5 connected to the domain who may have like weak passwords 6 or, you know, local administrators. That's what I was 7 referencing. 8 Q I think there was a particular system that you 9 -- that you mentioned. 10 A Again, I described that as a lab environment. 11 Q What is the -- what does that -- what were you 12 referring to when you referred to the lab environment? 13 A Environments where we have workstations and 14 servers are used to do testing. 15 Q Okay. And those were not connected to the 16 SolarWinds' Active Directory? 17 A Not that I can recall, no. 18 Q Was solarwinds123 used as the original 19 password for company-owned devices that were provided to 20 employees? 21 A I don't know if it was or was not. 22 Q Was solarwinds123 the password for the company 23 -- the company's Wi-Fi? 24 A I don't believe so, no. 25 Q Have you signed onto the company's Wi-Fi</p>	<p style="text-align: right;">Page 365</p> <p>1 engineering group. 2 Q Are you familiar with the phrase "hard coded 3 password"? 4 A I've heard the term before. 5 Q Do you have an understanding of what it means? 6 A In what context? 7 Q A password for a application or server. 8 A Yeah, in that context, it would be a 9 credential used and placed within product code, for 10 example, or a script, you know, that you're running. 11 Q And so what does -- what does that mean? 12 What's the impact of having a hard coded password and 13 product code? 14 A It allows the product function or processes 15 running within the application to authenticate without 16 any interaction. 17 Q Are you familiar with the phrase as it relates 18 to software applications, "default passwords"? 19 A As it relates to applications? 20 Q Yes. 21 A Yes, default passwords, yes, I'm familiar. 22 Q What is a -- what is a default password? 23 A In the context of products, it's typically 24 credentials that are used during the installation of a 25 product and then, you know, changed shortly afterwards.</p>

Page 422

1 Q And you know -- just looking at this and
 2 without those details in front of you, it was -- I was
 3 asking about the conclusion previously. Do you recall
 4 whether any analysis -- whether your team did any
 5 analysis to try to reach a conclusion about that? Did
 6 they do any analysis to try to figure out if this was
 7 the same vulnerability or a different vulnerability?
 8 A As with all other externally reported issues,
 9 we worked with the customers to try and verify,
 10 replicate, or recreate what they're reporting to us.
 11 Again, because we're following those same processes, our
 12 engineering teams would have attempted to recreate what
 13 this customer was reporting.
 14 Q I guess my question's a little bit different.
 15 What I was asking is so without -- without regard to
 16 any conclusions you reached about similarities between
 17 this attack and the DOJ attack, do you recall if your
 18 team did any analysis, your security team did any
 19 analysis to try to determine whether this was -- whether
 20 this involved the same vulnerability?
 21 A I don't have -- I don't have any recollection
 22 of that. The information we would have gotten would
 23 have come from the engineering teams, and then we would
 24 have compared that, but again, I don't have the details
 25 in front of me.

Page 423

1 Q I'm going to show you just one more -- one
 2 more document. If I can refer you to Exhibit 48.
 3 (SEC Exhibit No. 48 was marked for
 4 identification.)
 5 BY MR. NEY:
 6 Q Exhibit 48 is an exhibit that's
 7 architecture/engineering security vulnerability and
 8 incident review dated June 24th, 2020. If you flip
 9 through it, you'll see some of the same -- same
 10 dashboards or same type of dashboards that we looked at
 11 previously. First, let me ask: Are you familiar with
 12 these architecture/engineering security vulnerability
 13 and incident reviews?
 14 A Yes, I am familiar with it.
 15 Q Okay. And is this -- were these used in
 16 meetings that you would attend?
 17 A No, I don't believe these were meetings that I
 18 would have attended.
 19 Q Okay. How are you familiar with these
 20 reports?
 21 A I would have been asked to provide the BI
 22 reports that are shown in the exhibit.
 23 Q Okay. I just want to ask about one very small
 24 item in here. If you flip to the Bates page ending in
 25 6872, there's a year-to-date ITOM product review

Page 424

1 relating to security. Do you see that?
 2 A Yes.
 3 Q At the bottom of that page, there is an
 4 incident number, ITOM 2020570, and the description and
 5 the title says that SolarWinds Papertrail customer
 6 claims there's an attacker inside SolarWinds. Do you
 7 see that?
 8 A Yes.
 9 Q Do you have a recollection of that incident --
 10 that incident in -- what came of that incident?
 11 A I don't recall the details around that
 12 incident. Again, we can always reference back to the
 13 incident number in Confluence to get the details, but I
 14 don't -- I don't recall the details around it.
 15 Q Okay. And so with that incident number, then
 16 you could -- you could find that and see what you-all
 17 did and what you determined?
 18 A We would -- we would be able to look at the
 19 logs and see what types of investigative steps were
 20 taken.
 21 MR. NEY: Give me just a moment. I'm just
 22 going to see if there's any additional things. Let me
 23 just go ahead and ask that: Is there -- are there any
 24 additional questions that members of SEC team wanted to
 25 ask at this point?

Page 425

1 MR. BAKER: This is Mike, not from me. Thank
 2 you.
 3 MS. STONE: Not from me either, Brad. Thanks.
 4 MR. BRUTLAG: Not from me. Thank you.
 5 MR. NEY: Ken, any additional questions?
 6 MR. ZAVOS: I didn't have anything else.
 7 MR. NEY: Okay. Great. I think we are going
 8 to go ahead and wrap up for today. Mr. Quitugua, we
 9 have no further questions for you at this time. We may,
 10 however, call you to testify again in this
 11 investigation, and should that be necessary, we'll
 12 contact you through your counsel again.
 13 Before we close the record, do you wish to
 14 clarify anything with respect to the statements that
 15 you've made over the last two days?
 16 THE WITNESS: No.
 17 MR. NEY: Counsel, do you have any clarifying
 18 questions that you'd like to ask before we close for the
 19 day?
 20 MS. RIEWE: We do not.
 21 MR. NEY: We are off the record at 4:10 p.m.
 22 on September 1st, 2021.
 23 (Whereupon, at 4:10 p.m., the examination was
 24 concluded.)
 25 * * * * *

Page 426

PROOFREADER'S CERTIFICATE

1
2
3 In the Matter of: SOLARWINDS, INC.
4 Witness: Eric Quitugua
5 File No: C-08755-A
6 Date: Wednesday, September 1, 2021
7 Location: Chicago, Illinois
8

9 This is to certify that I, Christine Boyce,
10 (the undersigned) do hereby certify that the foregoing
11 transcript is a complete, true and accurate
12 transcription of all matters contained on the recorded
13 proceedings of the investigative testimony.
14
15
16
17
18

19 _____ 9-13-2021
20
21
22
23
24
25

Page 427

REPORTER'S CERTIFICATE

1
2
3 I, Kevin Carr, reporter, hereby certify that the
4 foregoing transcript is a complete, true and accurate
5 transcript of the testimony indicated, held on 9-1-21,
6 at Chicago, IL in the matter of:
7 SOLARWINDS, INC.
8

9 I further certify that this proceeding was recorded by
10 me, and that the foregoing transcript has been prepared
11 under my direction.
12
13
14

15 9-13-2021
16
17
18
19
20
21
22
23
24
25